CLAIMS

1. A method for secure key delivery for decrypting a distribution archive file at an unsecure site that receives a stream of distribution archive files from a publishing site, the method comprising:
   (a) extracting a scheduled key from a first distribution archive file in the stream;
   (b) using the retrieved scheduled key to decrypt the next distribution archive file in the stream following the first distribution archive file; and
   (c) repeating steps (a) and (b) for each distribution archive file in the stream.

2. The method of claim 1 further comprising:
   (d) receiving a scheduled key for the first distribution archive file in the stream from the publishing site.

3. The method of claim 1 wherein each distribution archive file comprises a plurality of encrypted content files and wherein the method further comprises:
   (d) encrypting, with a scheduled key, a distribution archive file including a scheduled key for the next distribution archive file in the stream and the plurality of encrypted content files.

4. The method of claim 1 wherein each distribution archive file comprises a plurality of encrypted content files and wherein the method further comprises:
   (d) encrypting, with a scheduled key, a distribution archive file including the plurality of encrypted content files and a non-encrypted scheduled key for the next distribution archive file.

5. The method of claim 1 wherein each distribution archive file comprises a plurality of digital content documents and the method further comprises:

(d) at the publishing site, encrypting each digital content document with a key to generate encrypted document content;

(e) at the publishing site, computing for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document;

(f) at the publishing site, creating a list of document identifier and decryption key pairs;

(g) at the publishing site, assembling the encrypted document content for each content document and the key pair list into a distribution archive file; and

(e) encrypting the distribution archive file with a scheduled key.

6. The method of claim 5 wherein step (g) comprises generating a new scheduled key, encrypting the new scheduled key and including the encrypted scheduled key in the distribution archive file.

7. The method of claim 6 wherein the new scheduled key is encrypted using a text string embedded in program code in the publishing site.

8. The method of claim 7 wherein step (a) comprises storing an extracted scheduled key in encrypted form.

9. The method of claim 8 wherein the extracted scheduled key is encrypted with a text string embedded in program code at the unsecure site.

10. The method of claim 9 wherein the text string embedded in program code in the publishing site is the same as the text string embedded in program code at the unsecure site.

11. Apparatus for secure key delivery for decrypting a distribution archive file at an unsecure site that receives a stream of distribution archive files from a publishing site, the apparatus comprising:

a key decryptor that extracts a scheduled key from each distribution archive file in the stream;

means for temporarily storing the extracted scheduled key; and

a decryption engine that uses the stored scheduled key to decrypt the next distribution archive file in the stream following the distribution archive file from which the scheduled key was extracted.

12. The apparatus of claim 11 further comprising means for receiving a scheduled key for the first distribution archive file in the stream from the publishing site.

13. The apparatus of claim 11 wherein each distribution archive file comprises a plurality of encrypted content files and wherein the apparatus further comprises an encryption engine that encrypts, with a scheduled key, a distribution archive file including a scheduled key for the next distribution archive file in the stream and the plurality of encrypted content files.

14. The apparatus of claim 11 wherein each distribution archive file comprises a plurality of encrypted content files and wherein the apparatus further comprises an encryption engine that encrypts, with a scheduled key, a distribution archive file including the plurality of encrypted content files and a non-encrypted scheduled key for the next distribution archive file.

15. The apparatus of claim 11 wherein each distribution archive file comprises a plurality of digital content documents and the apparatus further comprises:

at the publishing site, an encryption engine that encrypts each digital content document with a key to generate encrypted document content;

at the publishing site, an OID calculator that computes for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document;

at the publishing site, means for creating a list of document identifier and decryption key pairs;

at the publishing site, means for assembling the encrypted document content for each content document and the key pair list into a distribution archive; and

means for encrypting the distribution archive with a scheduled key.

16. The apparatus of claim 15 wherein the means for encrypting the distribution archive with a scheduled key comprises a key generator that generates a new scheduled key, a key encryptor that encrypts the new scheduled key and means for including the encrypted scheduled key in the distribution archive.

17. The apparatus of claim 16 wherein the key encryptor encrypts the new scheduled key using a text string embedded in program code in the publishing site.

18. The apparatus of claim 17 wherein the means for temporarily storing the extracted scheduled key comprises means for storing an extracted scheduled key in encrypted form.

19. The apparatus of claim 18 wherein the means for temporarily storing the extracted scheduled key comprises means for encrypting the extracted scheduled key with a text string embedded in program code at the unsecure site.

20. The apparatus of claim 19 wherein the text string embedded in program code in the publishing site is the same as the text string embedded in program code at the unsecure site.

21. A computer program product for secure key delivery for decrypting a distribution archive file at an unsecure site that receives a stream of distribution archive files from a publishing site, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code for extracting a scheduled key from each distribution archive file in the stream;

program code for temporarily storing the extracted scheduled key; and

program code for using the stored scheduled key to decrypt the next distribution archive file in the stream following the distribution archive file from which the scheduled key was extracted.

22. The computer program product of claim 21 further comprising program code for receiving a scheduled key for the first distribution archive file in the stream from the publishing site.

23. The computer program product of claim 21 wherein each distribution archive file comprises a plurality of encrypted content files and wherein the computer program product further comprises:

program code for encrypting, with a scheduled key, a distribution archive file including a scheduled key for the next distribution archive file in the stream and the plurality of encrypted content files.

24. The computer program product of claim 21 wherein each distribution archive file comprises a plurality of encrypted content files and wherein the computer program product further comprises:

program code for encrypting, with a scheduled key, a distribution archive file including the plurality of encrypted content files and a non-encrypted scheduled key for the next distribution archive file.

25. The computer program product of claim 21 wherein each distribution archive file comprises a plurality of digital content documents and the method further comprises:

program code at the publishing site, for encrypting each digital content document with a key to generate encrypted document content;

program code at the publishing site, for computing for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document;

program code at the publishing site, for creating a list of document identifier and decryption key pairs;

program code at the publishing site, for assembling the encrypted document content for each content document and the key pair list into a distribution archive file; and

program code for encrypting the distribution archive file with a scheduled key.

26. The computer program product of claim 25 wherein the program code for encrypting the distribution archive file comprises program code for generating a new scheduled key, program code for encrypting the new scheduled key and program code for including the encrypted scheduled key in the distribution archive file.

27. The computer program product of claim 26 wherein the program code for encrypting the new scheduled key encrypts the new scheduled key using a text string embedded in program code in the publishing site.

28. The computer program product of claim 27 wherein the program code for temporarily storing the extracted scheduled key comprises program code for storing an extracted scheduled key in encrypted form.

29. The computer program product of claim 28 wherein the program code for encrypting the extracted scheduled key encrypts the extracted scheduled key with a text string embedded in program code at the unsecure site.

30. The computer program product of claim 29 wherein the text string embedded in program code in the publishing site is the same as the text string embedded in program code at the unsecure site.